


Havells India
ISMS Manual

Version 1.2

Havells India Limited Havells India ISMS Manual Version 1.2 Internal	
---	---

Document Statistics

S. No.	Type of Information	Document Data
1.	Document Title	Havells ISMS Manual
2.	Document Code	HISMSM
3.	Date of Release	20 th Feb 2023
4.	Document Superseded	1.1
5.	Document Approvers	Mr. Pramod Mundra and Mr. Ramanand Jha
6.	Document Owner	Information Security Head
7.	Documents Author(s)	Mr. Sanjay Roongta and Mr. Neeraj Nagpal

Document Approvers

S. No.	Approver	Approver Designation	Approver Contact
1.	Pramod Mundra	Chief Information Officer (CIO)	Pramod.Mundra@havells.com
2.	Ramanand Jha	Information Security Head	ramanand.jha@havells.com

Document Change Approvals

Version No.	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	18th Feb 2022
1.1	26 th Feb 2022	Added IS objectives, Competency Matrix as part of annexure and updated section 2.3.2	27 th Feb 2022
1.2	20 th Feb 2023	IS objective is incorporated in ISMS Scope and Objectives_v1.2	20 th Feb 2023

Document Scope

This document shall be applicable to the IT Department and the employees/Third Parties referred henceforth shall include the staff working with IT department and/or handling, processing, and managing information/information assets of Havells.

Document Distribution

The Information Security Head shall distribute this policy to all employees working with IT department and/or handling, processing, and managing information/information assets of Havells by uploading it on the intranet/by sharing it via email/as appropriate.

Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

Table of Contents

1. Introduction	5
1.1. Havells India Limited.....	5
2. Planning ISMS.....	5
2.1. Establishing and managing ISMS	5
2.2. Internal and external issues	6
2.3. Provision of resources	7
2.4. ISMS Training and Awareness	13
2.5. Control of Documentation and Records	13
3. Implementing and Operating.....	14
3.1. Implementing and operating ISMS.....	14
3.2. Exercising and Testing.....	14
3.3. Monitoring and review	14
4. Maintaining and Improving the ISMS	15
5. Scope Exclusion and Justification for Scope Exclusion	15

1. Introduction

Havells India Limited recognizes the criticality and need of its business and understands the importance of IT security, confidentiality, integrity, and availability of its critical business processes that support the key products and services.

1.1. About Havells India Limited

Havells India Limited is a leading Fast-Moving Electrical Goods (FMEG) company and a major power distribution equipment manufacturer with a strong global presence. Havells has great market dominance across a wide spectrum of products.

The following is the input for scope definition for Havells India:

Department	Inputs for scope definition
Information Technology	The IT department shall be responsible for the following activities, but not limited to: <ul style="list-style-type: none">a) Devising and implementing the information security policies for the organizationb) Managing and maintaining the IT infrastructure of Havells and its Group companies;c) Maintaining applications that are being used by various business functions;d) Vendor management for development of software for maximizing the efficiency of operations and maintenance of applications; ande) Conducting independent assessment of Havells' security posture and providing inputs to the management on the key improvement areas.

Table 1: Input for scope definition

2. Planning ISMS

2.1. Establishing and managing ISMS

2.1.1 ISMS objectives and scope

. The scope of ISMS at Havells applies to the identified assets and locations for IT department. The information security requirements, scope and objectives have been identified in the Information Security Policy and ISMS Scope and Objectives document.

(Refer: Information Security Policy and ISMS Scope and Objectives)

2.1.2 ISMS Policy

The purpose of the ISMS policy is to establish the management's intent towards setting up and maintaining effective ISMS. The ISMS policy of Havells is developed to ensure the protection of its information assets and to allow the use, access, and disclosure of such information in accordance with appropriate standards, laws, and regulations.

The detailed policy domains are incorporated in "Havells Information Security Policy".

2.1.2 Legal and Regulatory Requirement

Havells India has a separate team to take care of statutory and regulatory requirements. Dedicated expertise is also line with respective functional team. Beside Legal, secretarial and Risk Management team.

(Refer: Functional SOP)

2.2. Internal and external Risks

Havells shall determine internal and external Risk that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

The below listed interested parties and internal & external issues of information security management system are relevant and can affect the achievement of the intended outcome of the program:

Interested Parties	Internal / External	Possible Risks
Employees and Management Staff	Internal	<ul style="list-style-type: none"> a) Non-availability of trained staff b) Dis-satisfied employees c) Lack-of inter departmental support d) Damage or destruction of personal assets
Personnel	Internal	<ul style="list-style-type: none"> a) Non-availability of management personnel b) Inefficient processes c) Compliance with the legal and regulatory requirements d) Loss of competitive advantage e) Service disruptions f) Any major incidents g) Mass churning of employees h) Non-availability of key employees
Internet / Network Services providers	External	<ul style="list-style-type: none"> a) Non-availability of internet / network service due to technical issue b) Non-availability of technical support c) Compromised quality of service d) Compromised SLAs/SLA breaches e) Breach in contract
IT Hardware, Software Supplies & Services	External	<ul style="list-style-type: none"> a) Non-availability of Hardware/Software/Applications / IT services due to technical issues b) Delay in the delivery/installation of infrastructure c) Delayed support services d) Compromised quality of deliverables e) Compromised quality of services f) Compromised SLAs/SLA breaches g) Lack of competent professionals h) Understaffed teams i) Breach in contract

Data center / DR Service	Internal / External	a) Non-availability of DC/DR services due to DC/DR Infrastructure services failures b) Inappropriate handling of infrastructure c) Lack of competent professionals d) Lack of appropriate physical security measures/controls e) Lack of appropriate infrastructure f) Compromised SLAs/SLA breaches g) Breach in contract h) Lack of appropriate business continuity measures/controls
Audits & Consultants	External	a) SLA breaches b) Lack in adherence to the timelines c) Understaffed teams
Infra-equipment Vendors	External	a) Lack of appropriate resources for providing services b) Lack of quality checks and testing c) Faulty devices/equipment d) SLA breach e) Lack of trained professionals for the equipment installation
Statutory Authorities	External	a) Inability to comply with the legal and statutory norms defined by these bodies

Table 2: Internal and external Risks

2.3. Provision of resources

Havells' management shall determine the roles needed to establish, implement, operate and maintain the ISMS.

- a) Management shall provide the nominations for the identified roles as per the required competency. Responsibilities and authorities of the resources shall be defined
- b) Management shall also be responsible for allocating required resources in terms of financial and funding allocations, any additional IT requirements, any facility related requirement (work location and infrastructure), any applications required to support the management systems and any additional training requirements etc.; and
- c) Management shall also determine the documents to be prepared or revised, and that supports the ISMS at Havells and shall ensure that these are available for use and reference with the required roles at all times.

Refer: HR SOP, Admin SOP

2.3.1. ISMS Governance Model

The governance framework for information security management system is defined below and includes the key roles and responsibilities during development and implementation of ISMS.

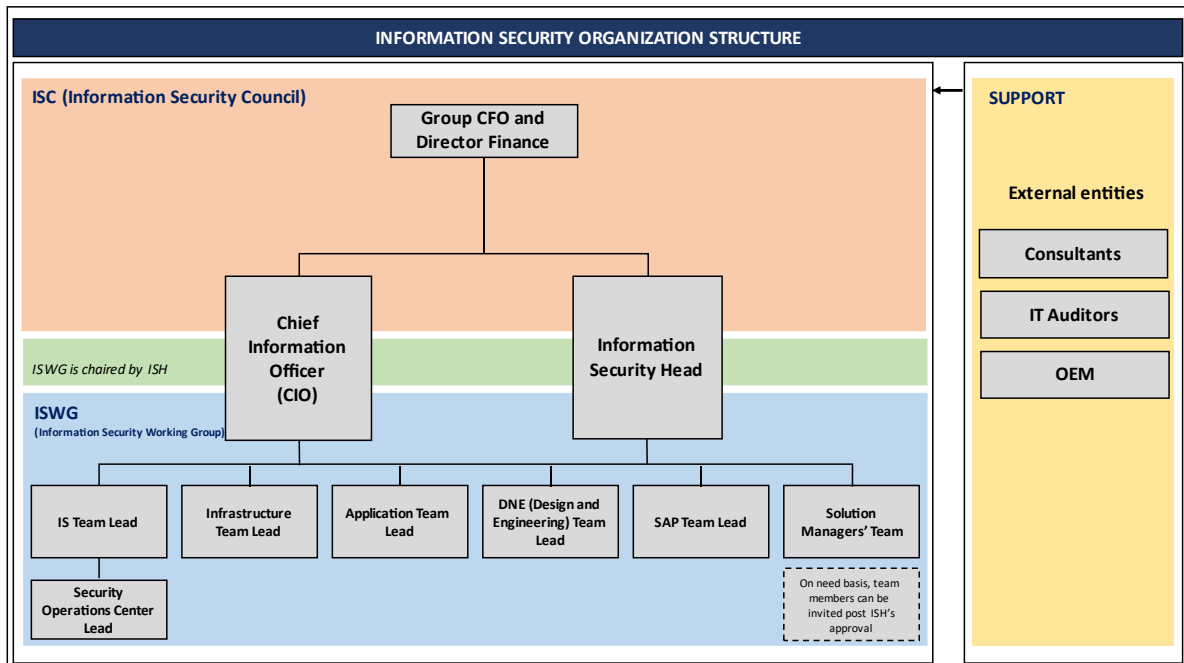


Figure 1: Information security organization structure

2.3.2. Information Security Roles, Responsibilities and Authorities

2.3.2.1. Information Security Council (ISC)

The ISC shall serve as a body providing strategic direction to securing Havells' information/data. The ISC would comprise of the following members such as:

- Group CFO and Director Finance
- Information Security Head;
- CIO/ Head of IT;

The responsibilities of the ISC are listed below, but not limited to:

- Provide information security directives across the IT department;
- Provide direction and support for the implementation of ISMS and constantly strive to improve the ISMS;
- Review and monitor major incident reports, together with the results of any investigation carried out;
- Guidance on information security education, training, and awareness;
- Ensure that employees are aware of their security roles and responsibilities;
- Review audit report on ISMS and follow-up on the status of corrective actions taken;
- To take care of legal and regulatory requirements of the organization pertaining to ISMS; and

The Information Security Council shall meet at least twice a year to assess the security requirements of Havells or as required by any significant change in the business operating environment.

2.3.2.2. Information Security Head

Havells, through its ISMS technical & management team, shall serve to provide strategic direction to securing Havells' information/data.

The responsibilities of Information Security Head are listed below, but not limited to:

- a) Accountability for oversight of the management of Information Security including the review and approval including assisting in the implementation of Havells' information security management system policies;
- b) Decide and approve the scope of Information Security Management System (ISMS);
- c) Ensure that Havells' processes integrate information security management systems requirements through a set of policies and procedures;
- d) Ensure the resources needed for ISMS are available;
- e) Periodically communicate the importance of ISMS and its conformance to employees;
- f) Monitor through periodic meetings & reviews that the intended outcomes of ISMS are achieved;
- g) Promote continual improvement of information security controls;
- h) Identify emerging trends in the industry vertical (within which the organization is currently poised), in relation to information safety and security measures;
- i) Point of contact to the department heads on information security implementation and non-compliances and to ensure that an effective process for implementing and maintaining the information security controls is in place;
- j) Ensure that the information security requirements for new information processing facilities have been identified and approved;
- k) Review and monitor major incident reports together with the results of any investigation carried out;
- l) Ensure that the policy is regularly reviewed and any recommendations to the same shall be reviewed with ISC;
- m) Encourage the participation of the managers, auditors, legal department, and the employees from various departments, who can contribute to compliance with information security practices;
- n) Coordinate any incident response procedures undertaken in response to potential information security breaches; and
- o) Ensure that adequate information security training is provided to various end users and Information Security Awareness programs are conducted regularly

2.3.2.3. IS Team Lead

IS team lead is the role defined for driving information security planning at Havells. IS team lead shall be nominated by CIO and Information Security Head. He/she shall have the capability to drive information security management system related activities.

The responsibilities of IS team lead are listed below, but not limited to:

- a) Is familiar with the Havells' ISMS policy and procedures;
- b) Ensures periodic review, update and approval of the information security documents;
- c) Controls the ISMS documents and records and performs vital record management, as applicable;
- d) Reports the results of performance evaluation to top management in management review meetings;
- e) Ensures implementation of an ISMS employee awareness program;
- f) Coordinate and manage internal audits, management reviews and execution of corrections and corrective actions;
- g) Regularly update the Information Security Head on the compliance and implementation of ISMS framework;
- h) Coordinate the review and update of ISMS deliverables, as per the defined frequency;
- i) Ensure that ISMS internal audits are conducted as per the defined frequency;
- j) Facilitate risk assessment and external audits;
- k) Track and facilitate closure of ISMS observations/ gaps/ non-conformities identified during the internal/ external audits;
- l) Ensures that ISMS implementation at Havells' conforms to the requirements of the leading international standards ISO 27001;
- m) Responsibility to plan and coordinate management review at the Havells;
- n) Collation of review and audit observations and results for management review at the Havells; and
- o) Documentation of results of the management reviews at Havells and maintenance of the records for the same.

2.3.2.4. Information Security Working Group (ISWG)

The Information Security Working Group (ISWG) is entrusted with the responsibility of managing security related operations and coordinating with the concerned team for implementation and maintenance of the ISMS. The ISWG will meet on quarterly basis for discussing, planning, and coordinating information security related activities. The ISWG shall be chaired by Information Security Head.

The ISWG shall comprise of following members such as:

- a) Information Security Head;
- b) CIO/ Head of IT;
- c) Lead from below listed teams:
 - i. IS team;
 - ii. Security Operations Center;
 - iii. Infrastructure Team;
 - iv. Applications Team;

- v. DNE (Design and Engineering);
- vi. SAP Team;
- vii. Solution managers' team; and
- d) Any business function team member required for a specific ISWG meeting can be invited, post Information Security Head's approval.

The responsibilities of team lead from ISWG are listed below, but not limited to:

- a) Assist in defining information security policies and procedures for use;
- b) Work with Information Security Head to ensure that an effective implementation of information security controls;
- c) Remain up to date on security trends and threats against the information assets
- d) ISWG shall be involved in planning and coordinating ISMS audit activities;
- e) The ISWG shall be involved in the formulation of the management's response to the audit findings and follow-up to ensure that the security controls and procedures, as required, are implemented within the stipulated time frame;
- f) Coordinate with SOC team, and apprise the Information Security Head of identified or potential security threats and vulnerabilities; and
- g) Ensure that periodic training and awareness programs are conducted to educate various end users (employees/third parties) on information security

Refer: DOA for Authorities

2.3.3. Competency of ISMS Personnel

Havells Information Security Council (ISC) shall ensure that all the ISMS roles identified are competent. The ISMS roles identified in the organization structure should be competent as per the below matrix.

Note: Following is the illustrative list. The final decision shall be as per Functional/Corporate HR's decision.

Information Security Council	
Competency Parameter	Competency Parameter
Academic	Graduate or post-graduate
Professional	<ul style="list-style-type: none"> a) Proven ability to successfully liaise and negotiate with a variety of people within all business functions and at all levels, both internal and external to organization; b) A decision maker; c) Sound understanding of the business model; d) Thorough knowledge of the company-wide ISMS; e) Adequate professional work experience; f) Effective written and verbal communication skills.
Behavioural	<ul style="list-style-type: none"> a) Should possess strong leadership skills; b) Should be able to lead in a complex and dynamic business environment; c) Should promote teamwork, quality, and efficiency and employee development.

Information Security Head	
Competency Parameter	Competency Details
Academic	Graduate or post-graduate
Professional	<ul style="list-style-type: none"> a) Understanding information security principles to build organizational policies and procedures of globally accepted ISO Standard 27001; b) Effective organizational skills; c) Thorough knowledge of the business; d) Understanding of business functions; e) In-depth understanding of the project delivery and the associated controls with respect to ISMS, and any other regulations; f) Effective project management skills; g) Rich professional work experience.
Behavioural	<ul style="list-style-type: none"> a) Should possess strong leadership skills; b) Should possess strong analytical abilities to identify, analyze and address information security risks; c) Should be able to lead in a complex and dynamic business environment.

IS team lead	
Competency Parameter	Competency Details
Academic	Graduate or post-graduate
Professional	<ul style="list-style-type: none"> a) In-depth understanding of information security management; b) Understanding information security principles to build organizational policies and procedures of globally accepted ISO 27001 standard; c) Good understanding of associated security controls with respect to ISMS, and other regulations; d) Effective project management skills; e) Technical work experience.
Behavioural	<ul style="list-style-type: none"> a) Should possess strong analytical abilities to identify, analyze and address information security risks; b) Should be able to lead in a complex and dynamic security environment.

ISWG team leads	
Competency Parameter	Competency Details
Academic	Graduate or post-graduate
Professional	<ul style="list-style-type: none"> a) Effective organizational skills; b) Understanding of business functions; c) In-depth understanding of the Project Delivery and the associated controls with respect to ISMS, and any other regulations; d) Effective project management skills; e) Related professional work experience.

Behavioural

- c) Should possess strong leadership skills;
- d) Should be able to lead in a complex and dynamic business environment.

2.4. ISMS Training and Awareness

Havells' management is determined to embed information security into its routine operations and management processes. This includes communicating information security policy to all employees and the importance of meeting information security objective and ensuring that all employees are aware of how they contribute to the achievement of the information security objectives. To achieve this Havells will raise, enhance, and maintain awareness through an ongoing ISMS training and awareness program for all employees and shall establish a process for evaluating its effectiveness.

2.5. Control of Documentation and Records

The ISMS framework at Havells has a set of policies to implement and maintain an effective ISMS. These policies are set of activities with defined outcome, deliverables, and evaluation criteria to attain information security on an ongoing basis.

ISMS Section	ISMS Document at Havells
ISMS Policy	Information Security Policy
ISMS Scope	ISMS Scope and Objectives
ISMS Supporting Policies	<ul style="list-style-type: none"> i. Acceptable Usage Policy ii. Access Control Policy iii. Asset Management Policy iv. Backup and Restoration Management Policy v. Change Management Policy vi. Security Exception management policy vii. Human Resource Security Policy viii. Incident Management Policy ix. ISMS Communication Policy x. ISMS Manual xi. Network Security Management Policy xii. Password Management Policy xiii. Physical Security Management Policy xiv. Risk Management, Risk Assessment and Recovery Strategy Procedure xv. System Acquisition and Development Policy xvi. Statement of Applicability xvii. Third Party Security Policy xviii. IT Continuity Policy

3. Implementing and Operating

3.1. Implementing and operating ISMS

3.1.1 Threat Assessment: Likelihood, Impact and Velocity

The Information Security Head would facilitate the threat assessment process and would work with the ISWG to identify threats that could exploit the vulnerability to impact the overall business processes of Havells (in terms of financial, operational, regulatory, and reputational).

(Refer: Risk Management, Risk Assessment and Recovery Strategy Procedure)

3.1.2 Risk Assessment

Risk assessment is a careful examination of threats that could cause harm, loss, or damage to assets of Havells. Risk Assessment will involve identification of threats, which could have an adverse impact on information assets and analysis of these threats to determine the likelihood of occurrence and their impact.

(Refer: Risk Management, Risk Assessment and Recovery Strategy Procedure)

3.1.3 Risk Treatment

Risk Treatment Plan (hereafter referred to as RTP) involves prioritizing, evaluating, and implementing appropriate controls as per the risk computation.

3.1.4 Developing and implementation of policies

The detailed policies are incorporated in “Information Security Policy”

Refer: Information Security Policy

3.2. Exercising and Testing

Havells’ management intends to exercise the arrangements for information security to provide greater assurance following an incident that critical activity will be recovered as required.

3.3. Monitoring and review

Management at Havells will monitor, review, and evaluate the effectiveness and efficiency of the ISMS, review the appropriateness of the information security policy, objectives, and scope, and determine and authorize actions for remediation and improvement. To ensure this, following activities will be undertaken at periodic basis:

- a) **Performance evaluation:** It is a self-evaluation process for the maintenance of ISMS which focuses on the measurement of the ISMS implementation effectiveness based on pre-defined KPI parameters. Each objective of Information Security is measured in performance evaluation. Performance evaluation process may get triggered as a result of changes in the organization or as per the audit outputs.
- b) **Internal audit:** Havells shall ensure that internal audits are conducted on a periodic basis to:
 - i. Determine whether the ISMS:

1. Conforms to planned arrangement for ISMS, including the requirements of the ISMS standard – ISO 27001:2013;
 2. Has been properly implemented and is maintained;
 3. Is effective in meeting the ISMS policy and objectives as documented;
- ii. Provide information on the results of the internal audits to the management.
- c) **Management Review:** Consists of Management Review and Third-Party Audits/internal independent auditors to monitor the established ISMS.

4. Maintaining and Improving the ISMS

Havells' management is determined to maintain and improve the effectiveness of the ISMS by taking actions, as determined by the monitoring and reviews. Improvements are planned against the non-conformities observed during third party audit, actions taken during and post incidents, post exercises, performance evaluation, internal and audits and management reviews.

Correction and corrective action shall be documented if following are observed:

- a) Nonconformities and observations received after internal/third party audits;
- b) Learnings from incidents;
- c) Post exercises planned as part of the training and awareness program; and
- d) Post management review.

5. Scope Exclusion and Justification for Scope Exclusion

The management of Havells has defined the scope exclusion and justification for scope exclusion. The decision of exclusion of scope has been approved by Information Security Head in consultation with Information Security Council (ISC).

(Refer: ISMS Scope & Objectives)



ISMS Manual-
Annexure-1 (Compe